AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS

16. (previously presented) A method for distributed remote network monitor (dRMON) in LAN comprising:

deploying dRMON agents that communicate with a dRMON proxy within ESs to be monitored, said dRMON agents implementing RMON functional groups but only capturing and analyzing packets that their native ES sends or receives;

on a periodic basis having the dRMON agents forward statistics and/or captured packets to said dRMON proxy, existing somewhere on the LAN; and

combining received agent data thereby creating at the dRMON proxy a view that a stand-alone RMON probe would have if all the ES were on the same LAN segment with it.

17. (currently amended) The method according to claim 16 wherein said dRMON proxy can mimic the SNMP responses of a prior art non-distributed RMON probe so that existing network application management software can interact with ~~the~~ said dRMON proxy as though said dRMON proxy were a probe.

18. (previously presented) The method according to claim 16 wherein in a default mode, ESs in the same multicast domain are treated by a dRMON proxy as though they are on one LAN segment to RMON applications that interact with the dRMON proxy though it were a

RMON probe and a user is provided with the ability to combine ports and hosts in order to create Virtual LAN (VLAN) definitions to cause the monitoring function to behave as though all selected hosts were on the same LAN segment being served by the same RMON probe with the dRMON proxy in this embodiment creating and maintaining several such views with each appearing as one interface to RMON Management applications.

19. (previously presented) The method according to claim 16 whereby said dRMON agents perform continual response time monitoring and forward the results to the dRMON Proxy.

20. (previously presented) The method according to claim 16 whereby said software utilizes native OS APIs to gather information about the ES that could not be gathered via packet capture and analysis, said information being selected from the group consisting of: (1) Network protocol stack configurations and NIC configurations including problematic situations; (2) Application information ranging from what protocols an application is bound to, to its manufacturer, version, file date and time, DLLs used and their versions; (3) System information such as memory, CPU, disk space, current resource utilizations; and (4) System performance metrics.